Detection and Response to Cybersecurity Threats on BC Hydro's Industrial Control Systems **Released [03/19]**

http://www.bcauditor.com/pubs

PAC Meeting Plan[1]	**[12/09/19]**	**Prepared by: Kip Morison, Paul Choudhury, BC Hydro**	**Reviewed by: Les MacLaren, ADM, EMPR**
1st APPA Update	**[19/02/20]**	**Prepared by: Kip Morison, BC Hydro**	**Reviewed by: Les MacLaren, ADM, EMPR**
2nd APPA Update	**[23/02/21]**	**Prepared by: Kip Morison, BC Hydro**	**Reviewed by: Les MacLaren, ADM, EMPR**

[1] The audited organization will be required to present their initial action plan at this meeting (i.e. First three columns completed for each OAG recommendation included in the audit report)

Please provide your email response to:

Email: Comptroller General's Office of the Government of British Columbia Comptroller.General@gov.bc.ca

Cc email to: the Office of the Auditor General of British Columbia actionplans@bcauditor.com

Rec. # Accepted? Yes / No[2]	OAG Recommendations	Actions Planned & Target Date(s)[3]	Assessment of Progress to date[4] and Actions Taken[5] (APPA update)
1 Yes	We recommend that BC Hydro assess cybersecurity risk over its entire industrial control systems (ICS) environment to ensure appropriate detection and response measures are implemented.	BC Hydro is extending its assessment of cyber security risks to areas of the power system not already covered by mandatory standards and legal requirements in British Columbia. BC Hydro will use a risk based approach to prioritize mitigation measures where needed. An external consultant has been retained to develop a prioritized list of stations that would benefit from the Auditor General's recommendations as well as cyber security additions that are already being planned for compliance with future mandatory reliability standards. Site visits to representative substations were completed in June and July 2019, and risk assessment workshops held in August 2019. Following the risk assessment workshops, BC Hydro accepted delivery of a report with findings, recommendations, and a prioritized remediation plan in October 31, 2019. A multi-year program is proposed with target plans for the number of stations to be addressed each year. **Revised (Feb 2021)** Due to an urgent focus on addressing Mandatory Reliability Standards (MRS) compliance issues and delays caused by COVID-19 the completion date for the development of the multi-year program plan has been extended to May 2021. **Revised Target Dates:** Start date April 1, 2019 – completion May 2021.	**Substantially implemented**. A risk assessment report of a representative sample of BC Hydro's industrial control systems (ICS) was completed and delivered to BC Hydro in October 2019. The report was summarized and presented to BC Hydro's executive team in November 2019. BC Hydro used a risk based approach to remediate several of the vulnerabilities identified in the assessment report. These actions included the addition of firewalls at some key locations and a process to monitor them. BC Hydro is using the 2019 report and previously assessed measure of criticality of its stations to complete the program plan and initiate the multi-year program that will address the highest risk facilities that are not covered by previous mandatory standards. Based on initial planning completed under BC Hydro's NERC CIP v7 project to implement NERC Critical Infrastructure Protection (CIP) v7 Standards (low impact stations), BC Hydro plans to coordinate work to address the Audit with the project work currently underway. NERC CIP v7 will address MRS compliance at approximately 130 low impact stations and involves completing an inventory (by June 2021), development of a cyber and physical reference architecture (by June 2021), and implementation of the controls (by end of 2023). These are the same basic steps required to meet the Audit recommendation. BC Hydro plans to use the same methodology, tools and reference architecture to implement inventory collection and detection/response capabilities for stations not covered by CIP standards but identified as high risk. There are approximately 150 stations that will be assessed for risk and implementation will follow completion of NERC CIP v7 implementation.

[2] For each recommendation, the audited organization should state whether or not they have accepted the recommendation and plan to implement it fully by typing either "Yes" or "No" under the number of the recommendation.
[3] Target date is the date that audited organization expects to have "fully or substantially implemented" the recommendation. If several actions are planned to implement one recommendation, indicate target dates for each if they are different.
[4]The Select Standing Committee on Public Accounts (PAC) will request that the audited organization provide a yearly update (i.e. completed "Assessment of Progress and Actions Taken" column) until all recommendations are fully implemented or otherwise addressed to the satisfaction of the PAC. This is for the APPA update.
[5] This action plan and the subsequent updates have not been audited by the OAG. However, at a future date that Office may undertake work to determine whether the entity has implemented the recommendations. The results of that work will be reported in a separate report prepared by the OAG.

Please provide your email response to:
Email: Comptroller General's Office of the Government of British Columbia Comptroller.General@gov.bc.ca
Cc email to: the Office of the Auditor General of British Columbia actionplans@bcauditor.com

Rec. # Accepted? Yes / No[2]	OAG Recommendations	Actions Planned & Target Date(s)[3]	Assessment of Progress to date[4] and Actions Taken[5] (APPA update)
2. Yes	We recommend that BC Hydro maintain an inventory of hardware and software components, including their configuration, settings for all ICS-related systems and devices, regardless of whether they currently fall under the mandatory standards	Based on the risk assessment and program development activities resulting from recommendation #1, BC Hydro will develop plans and cost estimates for building inventories at stations where there are gaps. The work associated with building missing inventories will be coordinated with actions resulting from recommendation #3 for efficiency reasons. All expenditures associated with these actions will be subject to BCUC approval. **Revised (Feb 2021)** Due to an urgent focus on addressing Mandatory Reliability Standards (MRS) compliance issues and delays caused by COVID-19 the start date for this work has been delayed to April 2021 and will continue on an ongoing basis for several years. Work on non-NERC stations is expected to follow the completion of the implementation of NERC CIP v7 (low impact facilities) standards. **Revised Target Dates:** Start date April 2021– completion Dec 31, 2025	**Partially implemented**. BC Hydro is reviewing its procedures, tools and systems for maintaining inventory, including configuration settings, for systems and devices that currently fall under mandatory standards as part of the work to address MRS. Work required to implement NERC CIP v7 Standards will inventory low impact stations and will include the development of a reference architecture for cyber and physical security. CIP v7 implementation will be completed by 2023. BC Hydro expects to extend, where technically feasible, the use of this approach for maintaining inventory, including configuration settings to ICS-related systems which do not fall under mandatory standards over the course of the remediation program resulting from recommendation #1.

Rec. # Accepted? Yes / No[2]	OAG Recommendations	Actions Planned & Target Date(s)[3]	Assessment of Progress to date[4] and Actions Taken[5] (APPA update)
3. Yes	We recommend that BC Hydro implement detection mechanisms and monitor, in real time, for anomalous activity on ICS-related systems and devices not currently under the mandatory standards.	Based on the risk assessment and program development activities resulting from recommendation #1, BC Hydro will develop plans and cost estimates for implementing detection and monitoring mechanisms at stations where there are gaps and where it is technically feasible to do so. These actions will be coordinated with those resulting from recommendation #2 for efficiency reasons. All expenditures associated with these actions will be subject to BCUC approval. **Revised (Feb 2021)** Due to an urgent focus on addressing Mandatory Reliability Standards (MRS) compliance issues and delays caused by COVID-19 the start date for this work is now April 2021 and will continue on an ongoing basis for several years. Work on non-NERC stations is expected to follow the completion of the implementation of NERC CIP v7 (low impact facilities) standards. **Revised Target Dates:** Start date April 2021 – completion Dec 31, 2025	**Partially implemented**. BC Hydro used a risk based approach to remediate several of the vulnerabilities identified in the assessment report provided under recommendation #1. These actions included the addition of firewalls at some key locations and a process to monitor them. Detection and monitoring capability will be implemented, where it is technically feasible to do so, for ICS which do not fall under mandatory standards. This work will be implemented in conjunction with the remediation program resulting from recommendation #1.

Please provide your email response to:
Email: Comptroller General's Office of the Government of British Columbia Comptroller.General@gov.bc.ca
Cc email to: the Office of the Auditor General of British Columbia actionplans@bcauditor.com